Math 357
Expositional homework 03

Assigned: 2024–02–07 (W)
Due: 2024–02–19 (M)

The goal of this homework is to practice and extend our irreducibility–detector toolkit. The exercises are adapted from Dummit & Foote, 3e, Section 9.4.

Let t be an indeterminate; let $\mathbf{Z}$ denote the ring of integers; and for $p \in \mathbf{Z}$ prime, let $\mathbf{F}_p = \mathbf{Z}/(p)$ (a finite field with p elements).

(a) Prove the Eisenstein–Schönemann criterion for $\mathbf{Z}$, as we stated it in class: Let $p \in \mathbf{Z}$ be prime; let $f = a_n t^n + \ldots + a_0 \in \mathbf{Z}[t]$, with $n = \deg f \geqslant 1$; and let $p \nmid a_n$, $p \mid a_{n-1}, \ldots, a_0$, and $p^2 \nmid a_0$. Then f is irreducible in $\mathbf{Q}[t]$. Moreover, if $\gcd(a_n, \ldots, a_0) = 1$, then f is irreducible in $\mathbf{Z}[t]$.

(b) For each of the following polynomials, determine whether it is irreducible or reducible in the indicated polynomial ring. If it is reducible, then give its factorization into irreducibles.

$$f(t) = t^6 + 30t^5 - 15t^3 + 6t - 120 \in \mathbf{Z}[t]$$
$$g(t) = t^3 + t + 1 \in \mathbf{Z}[t]$$
$$h(t) = t^3 + t + 1 \in \mathbf{F}_3[t]$$

(c) Let $n \in \mathbf{Z}_{>0}$, and consider the polynomial

$$f_n(t) = 1 + \prod_{i=1}^{n} (t - i) \in \mathbf{Z}[t]$$

Show that f_n is irreducible for all $n \neq 4$.

(d) Let $p \in \mathbf{Z}$ be prime, and consider the cyclotomic polynomial[1]

$$\Phi_p(t) = t^{p-1} + \ldots + 1 \in \mathbf{Z}[t]$$

Show that Φ_p is irreducible. Explain the technique you use. *Hint:* See p 310.

(e) Let F be a field, let $f \in F[t]$, and let $n = \deg f$. The **reverse** of f is the polynomial $t^n f(t^{-1})$. Justify why this construction gives a valid polynomial in $F[t]$ (even though t^{-1} is not an element of $F[t]$). Give an example of a polynomial and its reverse that clearly illustrates why this name is apt for this construction. Prove that if $f(0) \neq 0$, then f is irreducible if and only if its reverse is irreducible.

[1] Note that we can view Φ_p as the quotient of $t^p - 1$ when (evenly) divided by $t - 1$; that is, $\Phi_p(t) = \frac{t^p - 1}{t - 1}$.

Solutions

Exercise (a)

Suppose for the sake of contradiction that f is reducible in $\mathbf{Q}[t]$. Then by Gauss's lemma, f is reducible in $\mathbf{Z}[t]$, say

$$f = f_1 f_2 \tag{1}$$

with $\deg f_i \geqslant 1$.[2] Given a prime $p \in \mathbf{Z}$, let

$$\varphi_p : \mathbf{Z}[t] \to (\mathbf{Z}/(p))[t]$$

be the reduction homomorphism associated to the prime ideal (p) in $\mathbf{Z}$, which sends a polynomial $g \in \mathbf{Z}[t]$ to the polynomial $\overline{g} = \varphi_p(g) \in (\mathbf{Z}/(p))[t]$ whose coefficients are those of g reduced modulo p. Using (i) the fact that φ_p is a ring homomorphism and (ii) the hypotheses on the coefficients of f, we get

$$\overline{f}_1 \overline{f}_2 = \varphi_p(f_1)\varphi_p(f_2) = \varphi_p(f_1 f_2) = \varphi_p(f) = \overline{a}_n t^n$$

with $\overline{a}_n \neq 0$ in $\mathbf{Z}/(p)$. Thus $\overline{f}_1$ and $\overline{f}_2$ divide $\overline{a}_n t^n$ in $(\mathbf{Z}/(p))[t]$. Because (p) is a prime (in fact, maximal) ideal in $\mathbf{Z}$, $\mathbf{Z}/(p)$ is an integral domain (in fact, a field), so $(\mathbf{Z}/(p))[t]$ is an integral domain. Therefore, the constant term of both $\overline{f}_1, \overline{f}_2 \in (\mathbf{Z}/(p))[t]$ is 0, which is true if and only if the constant term of both $f_1, f_2 \in \mathbf{Z}[t]$ is divisible by p. This implies that the constant term of $f = f_1 f_2$ is divisible by p^2, a contradiction. We conclude that f is irreducible in $\mathbf{Q}[t]$.

Further suppose that the greatest common divisor of the coefficients of f is 1. Recall Corollary 9.6 (p 304):

> Let R be a unique factorization domain, let $F = \operatorname{Frac} R$, let $f \in R[t]$, and suppose that the greatest common divisor of the coefficients of f is 1. Then f is irreducible in $R[t]$ if and only if f is irreducible in $F[t]$.

We have just shown that f is irreducible in $\mathbf{Q}[t] = (\operatorname{Frac} \mathbf{Z})[t]$. Because $\mathbf{Z}$ is a euclidean domain, it is a unique factorization domain, and hence $\mathbf{Z}[t]$ is a unique factorization domain.[3] Hence Corollary 9.6 applies, and f is irreducible in $\mathbf{Z}[t]$.

Exercise (b)

We analyze each polynomial in turn.

$f = t^6 + 30t^5 - 15t^3 + 6t - 120 \in \mathbf{Z}[t]$ is irreducible by the Eisenstein–Schönemann criterion with the prime $p = 3$. In particular, 3 does not divide the leading coefficient of f, 3 divides all other coefficients of f, and 3^2 does not divide the constant term of f.

$g = t^3 + t + 1 \in \mathbf{Z}[t]$ is irreducible. We give two proofs. Both use the fact that a polynomial of degree 2 or 3 over a field is reducible if and only if its associated function has a zero.[4]

[2] See DF3e, Proposition 9.5, pp 303–4.

[3] See DF3e, Corollary 9.8, p 305.

[4] See DF3e, Proposition 9.10, p 308.

1. Method 1: Reduction modulo a proper ideal. Consider the maximal ideal $(2) \trianglelefteq \mathbf{Z}$ and the associated reduction homomorphism $\varphi_2 : \mathbf{Z}[t] \to (\mathbf{Z}/(2))[t]$. The polynomial

$$\varphi_2(g) = t^3 + t + 1 \in (\mathbf{Z}/(2))[t]$$

has no zeros in the field $\mathbf{Z}/(2)$, so $\varphi_2(g)$ is irreducible, and therefore g is irreducible.[5]

Note that the reduction part of this argument requires only a proper, not necessarily maximal, ideal. However, the equivalence of reducibility and zeros for degree-2 and degree-3 polynomials requires that the ring of coefficients be a field, which (for a quotient ring) requires that the ideal by which we quotient be maximal.

2. Method 2: Analysis in $\mathbf{Q}[t]$. View $g \in \mathbf{Q}[t]$. Because $\deg g = 3$, the polynomial g is reducible if and only if the induced function $g : \mathbf{Q} \to \mathbf{Q}$ has a zero. By the rational zeros test, if $\frac{a}{b} \in \mathbf{Q}$ is a zero of g with $\gcd(a, b) = 1$ (that is, $\frac{a}{b}$ is in lowest terms), then a divides the constant term of g and b divides the leading coefficient of g; that is, $a \mid 1$ and $b \mid 1$, so $\frac{a}{b} = \pm 1$. We compute

$$g(-1) = -1 \qquad\qquad g(1) = 3$$

We conclude that g is irreducible in $\mathbf{Q}[t]$. Because the greatest common divisor of the coefficients of g is 1, if g is irreducible in $\mathbf{Q}[t]$, then g is irreducible in $\mathbf{Z}[t]$, as desired.

$h = t^3 + t + 1 \in \mathbf{F}_3[t]$ is reducible. Because $\deg h = 3$, the polynomial h is reducible if and only if the induced function h has a zero. We compute that $h(1) = 0$, so h is reducible.

Exercise (c)

Suppose for the sake of contradiction that f_n is reducible in $\mathbf{Z}[t]$, say

$$f_n = g_1 g_2$$

Without loss of generality, let $\deg g_1 \leqslant \deg g_2$. By definition of f_n, $\mathrm{LC}(f_n) = 1$, so the greatest common divisor of the coefficients of f_n equals 1, and therefore each g_i has degree at least 1.

Note that

$$g_1 g_2 - 1 = f_n - 1 = \prod_{i=1}^{n} (t - i)$$

This implies that for each $\alpha \in \{1, \ldots, n\}$,

$$(g_1 g_2 - 1)(\alpha) = 0 \qquad \Leftrightarrow \qquad g_1(\alpha) g_2(\alpha) = 1 \qquad \Leftrightarrow \qquad g_1(\alpha), g_2(\alpha) = \pm 1$$

where in the final statement, for each α, $g_1(\alpha)$ and $g_2(\alpha)$ have the same sign. Denote

$$S_1 = \{\alpha \in \{1, \ldots, n\} \mid g_i(\alpha) = 1\} \qquad\qquad S_{-1} = \{\alpha \in \{1, \ldots, n\} \mid g_i(\alpha) = -1\}$$

Note that $S_1 \cup S_{-1} = \{1, \ldots, n\}$, so at least one of S_1, S_{-1} has order greater than or equal to $\lceil \frac{n}{2} \rceil$. Denote this set by S_M, where $M = \pm 1$.

[5] The last implication uses DF3e Proposition 9.12, p 309.

By hypothesis, $f_n = g_1 g_2$. Because $\mathbf{Z}$ is an integral domain, $\mathbf{Z}[t]$ is an integral domain, so

$$n = \deg f_n = \deg(g_1 g_2) = \deg g_1 + \deg g_2$$

Thus at least one of the g_i has degree less than or equal to $\lfloor \frac{n}{2} \rfloor$. Earlier we arranged that $\deg g_1 \leqslant \deg g_2$, so we have $\deg g_1 \leqslant \lfloor \frac{n}{2} \rfloor$.

Suppose $\deg g_1 < \frac{n}{2}$. Then the polynomial $g_1 - M$, which we may view in $\mathbf{Q}[t]$, has degree

$$\deg(g_1 - M) = \deg g_1 < \frac{n}{2}$$

and at least $\#(S_M) \geqslant \lceil \frac{n}{2} \rceil \geqslant \frac{n}{2}$ zeros, a contradiction. When n is odd, necessarily $\deg g_1 < \frac{n}{2}$. Thus this contradiction shows that if n is odd, then f_n is irreducible.

This contradiction also shows that if n is even, then we must have $\deg g_1 = \deg g_2 = \frac{n}{2}$ and $\#(S_1) = \#(S_2) = \frac{n}{2}$. In this case, the set S_1 contains $\frac{n}{2}$ distinct zeros for the degree-$\frac{n}{2}$ polynomial $g_i - 1$, for $i \in \{1, 2\}$. (The analogous statement holds for the set S_{-1} and the polynomial $g_i + 1$.) Therefore, for $i \in \{1, 2\}$,

$$g_i = -1 + \prod_{\alpha \in S_1} (t - \alpha) = 1 + \prod_{\alpha \in S_{-1}} (t - \alpha)$$

In particular, $g_1 = g_2$; denote the common polynomial by g. Thus

$$g^2 = f_n = 1 + \prod_{i=1}^{n} (t - i)$$

That is, if the polynomial f_n is reducible in $\mathbf{Z}[t]$, then it is a square. If we can show that the corresponding function f_n evaluates to negative values, then we will have a contradiction.

View the polynomials in $\mathbf{Q}[t]$, and consider evaluating their functions at $t = n - \frac{1}{2}$:

$$\left(g\left(n - \frac{1}{2}\right)\right)^2 = g^2\left(n - \frac{1}{2}\right) = f_n\left(n - \frac{1}{2}\right) = 1 + \left(-\frac{1}{2}\right) \prod_{i=1}^{n-1} \left(n - \frac{1}{2} - i\right) \tag{2}$$

If $n > 4$, then the product in this expression satisfies

$$\prod_{i=1}^{n-1} \left(n - \frac{1}{2} - i\right) = \left(\frac{1}{2}\right)\left(\frac{3}{2}\right)\left(\frac{5}{2}\right)\left(\frac{7}{2}\right) \cdots \left(n - \frac{1}{2} - 1\right) > \frac{105}{16} > 2$$

where we obtain the penultimate inequality by keeping only the first four factors and noting that any subsequent factors are greater than or equal to 1. Substituting this result into equation (2), it follows that if $n > 4$, then

$$\left(g\left(n - \frac{1}{2}\right)\right)^2 < 1 - \frac{1}{2}(2) = 0$$

a contradiction (recall that we are viewing g as a function from $\mathbf{Q}$ to $\mathbf{Q}$).

It remains to address the cases $n = 2$ and $n = 4$.

When $n = 2$,

$$f_2(t) = t^2 - 3t + 3$$

which is irreducible by the Eisenstein–Schönemann criterion with $p = 3$.

When $n = 4$,

$$f_4(t) = t^4 - 10t^3 + 35t^2 - 50t + 25 = (t^2 - 5t + 5)^2$$

so f_4 is reducible.

Exercise (d)

Note that we cannot apply the Eisenstein–Schönemann criterion directly to $\Phi_p(t)$. However, we compute

$$\begin{aligned}\Phi_p(t+1) &= \frac{(t+1)^p - 1}{(t+1) - 1} \\ &= t^{p-1} + pt^{p-2} + \ldots + \frac{p(p-1)}{2}t + p\end{aligned}$$

We note two aspects. First, the constant term in the numerator, before dividing by t in the denominator, is zero. Second, the coefficients of the final polynomial are $\binom{p}{i} = \frac{p(p-1)\cdots(p-i+1)}{i!}$, for $i \in \{0, \ldots, p-1\}$; in particular, all coefficients except the leading coefficient (corresponding to $i = 0$) are divisible by p. Thus we may apply the Eisenstein–Schönemann criterion with the prime p to $\Phi_p(t+1)$ to conclude that $\Phi_p(t+1)$, and hence $\Phi_p(t)$, is irreducible.

Exercise (e)

Let

$$f = a_n t^n + \ldots + a_0$$

By definition, its reverse is

$$\operatorname{rev} f = t^n f(t^{-1}) = t^n(a_n t^{-n} + \ldots + a_0) = a_n + \ldots + a_0 t^n$$

Because each monomial term in $f(t^{-1})$ has the form $a_i t^{-i}$ for some $i \in \{0, \ldots, n\}$, it follows that each monomial term in $t^n f(t^{-1})$ has the form $a_i t^{n-i}$, with $n - i \geqslant 0$. Thus this construction gives a polynomial in $F[t]$.

As an example, consider the polynomial

$$f = t^3 + 2t + 3$$

in $\mathbf{Q}[t]$. Then

$$\operatorname{rev} f = t^3 f(t^{-1}) = 1 + 2t^2 + 3t^3 = 3t^3 + 2t^2 + 1$$

This construction "reverses" the order of the coefficients of f relative to the powers of t.

Note that this construction can product a polynomial of strictly smaller degree than the input. More precisely, $\deg \operatorname{rev} f < \deg f$ if and only if the constant term of f is 0—that is, if and only if $f(0) \neq 0$. For example, if $f = t$, then $\operatorname{rev} f = 1$.

Let $f \in F[t]$, and suppose that $f = g_1 g_2$ for some $g_i \in F[t]$. Then a bookkeeping exercise with the definition of multiplication of polynomials shows that

$$(\operatorname{rev} g_1)(\operatorname{rev} g_2) = \operatorname{rev} f$$

Because the reverse of the reverse of a polynomial is the original polynomial, the reverse implication also holds.

Further suppose that $f(0) \neq 0$. Then because F is a field (and hence an integral domain), each g_i in the factorization $f = g_1 g_2$ satisfies $g_i(0) \neq 0$. In particular, if $g_i(0) \neq 0$ and $\deg g_i \geqslant 1$, then $\deg(\operatorname{rev} g_i) \geqslant 1$. It follows that such an f is reducible if and only if $\operatorname{rev} f$ is reducible.